IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1-20 (Canceled)

21. (New) A method for authenticating code modules on a computing device comprising:

receiving a code module into the computing device via a media interface;

loading the code module into a private memory of the computing device;

accessing a key embedded in the computing device in one of a processor, a chipset or a physical token; and

authenticating the code module in the private memory using the embedded key.

22. (New) The method of claim 21, further comprising:

locking the private memory.

23. (New) The method of claim 21, wherein authenticating the code module using the embedded key further comprises:

extracting a signature from the code module;

hashing a portion of the code module to obtain a computed digest value;

decrypting the signature using the embedded key to obtain a decrypted digest value;

determining whether the code module is authentic, wherein determining includes comparing the computed digest value to the decrypted digest value.

24. (New) The method of claim 21, further comprising:

updating security aspects of the computing device, if the code module is authentic; and

initiating execution of the code module, only if the code module is authentic.

25. (New) The method of claim 21, further comprising before loading the code module:

verifying the computing device possesses a proper environment;

locking a processor bus;

configuring the private memory; and

updating events processing.

26. (New) The method of claim 21, further comprising after the code module has executed:

reconfiguring the private memory;

updating security aspects of the computing device;

releasing the processor bus;

updating events processing;

terminating the code module; and

launching post code module code.

27. (New) An article of manufacture comprising a computer-readable medium having content stored thereon to provide instructions to result in a computing device performing operations including:

receiving a code module into the computing device via a media interface;

loading the code module into a private memory of the computing device;

accessing a key embedded in the computing device in one of a processor, a chipset or a physical token; and

authenticating the code module in the private memory using the embedded key.

28. (New) The article of manufacture of claim 27, further having content to provide instructions to result in the electronic device performing additional operations including:

locking the private memory.

29. (New) The article of manufacture of claim 27, wherein the instructions that when executed by a computing device cause the device to perform the operation of authenticating the code module using the embedded key further cause the device to perform additional operations including:

extracting a signature from the code module;

hashing a portion of the code module to obtain a computed digest value;

decrypting the signature using the embedded key to obtain a decrypted digest value;

determining whether the code module is authentic, wherein determining includes comparing the computed digest value to the decrypted digest value.

30. (New) The article of manufacture of claim 27, further having content to provide instructions to result in the electronic device performing additional operations including:

updating security aspects of the computing device, if the code module is authentic; and

initiating execution of the code module, only if the code module is authentic.

31. (New) The article of manufacture of claim 30, further having content to provide instructions to result in the electronic device performing additional operations before loading the code module including:

verifying the computing device possess a proper environment;

locking a processor bus;

configuring the private memory; and

updating events processing.

32. (New) The article of manufacture of claim 31, further having content to provide instructions to result in the electronic device performing additional operations after loading the code module including:

reconfiguring the private memory;

updating security aspects of the computing device;

releasing the processor bus;

updating events processing;

terminating the code module; and

launching post code module code.

33. (New) An apparatus comprising:

a private memory; and

a processor coupled with the private memory to load a code module into the private memory and to authenticate the code module using a key embedded in one of the processor, a chipset and a physical token.

34. (New) The apparatus of claim 33, further comprising:

a media interface coupled with the processor to receive the code module and send the code module to the processor.

35. (New) The apparatus of claim 33, wherein the private memory is part of the processor..

36. (New) The apparatus of claim 33, wherein the private memory is part of a cache memory that is part of the processor.

37. (New) The apparatus of claim 33, wherein the private memory is coupled to the processor via a dedicated data bus.

38. (New) The apparatus of claim 33, wherein the private memory is part of a main memory coupled to the process via a memory controller.

39. (New) The apparatus of claim 33, wherein the private memory is separate from the processor and coupled to the processor via a private memory controller that does not control a main memory.

40. (New) The apparatus of claim 33, wherein the private memory to clear before the code module is loaded, to lock after the code module is loaded, to clear after the code module has executed.